Journal of Industrial Information Integration 000 (2017) 1–14

Contents lists available at ScienceDirect

Journal of Industrial Information Integration

journal homepage: www.elsevier.com/locate/jii

Design and implementation of UPnP-based energy gateway for demand side management in smart grid

Rafiullah Khan[a,*], Sarmad Ullah Khan[b]

[a] Queen's University Belfast, BT7 1NN Belfast, United Kingdom
[b] Politecnico Di Torino, 10129 Turin, Italy

ARTICLE INFO

Article history:
Received 23 March 2017
Revised 24 June 2017
Accepted 12 July 2017
Available online xxx

Keywords:
Smart grid
Home energy gateway
Universal plug & play
Utility services
Demand side management
Smart home
Privacy
Security

ABSTRACT

Legacy electrical grids are urged to evolve towards smart grids, the smarter power delivery system that relies heavily on ICT. Numerous smart grids applications are expected to be developed for efficient management and utilization of electricity at the demand side such as home automation, Advanced Metering Infrastructure (AMI), dynamic energy pricing, efficient load management, etc. For easing and boosting the development of new demand side services, the concept of Home Energy Gateway (HEG) has recently been proposed in literature. It involves communication with the utility as well as with devices at the consumer sites. The literature still lacks a comprehensive HEG design that could provide all essential features such as zero-configuration, auto-discovery, seamless plug & play communication, interoperability and integration, customers privacy and communication security.

This paper addresses the HEG challenges in an effective way through the design of suitable communication frameworks and a security mechanism for enabling strong protection against cyber attacks. The proposed system effectively copes with the interoperability and integration issues between plethora of heterogeneous devices at the consumer sites. The devices in proposed system inherit plug & play features and support zero-configuration and seamless networking. Further, the proposed system design is technology-agnostic and flexible enough to be adopted for the implementation of any specific demand side service. This paper also evaluates the proposed system in real-networking environment and presents performance metrics.

1. Introduction

Today, efficient production, transmission and consumption of electricity are becoming increasingly important due to fossil resources depletion, ever rising cost of electricity and environmental concerns [1]. Further, legacy grids have several limitations which hinder the integration of renewable energy sources. The evolution of legacy grids towards smart grids brings more intelligence for efficient Demand Side Management (DSM) by massive integration of ICT. The use of ICT enables the development of more advanced DSM services which could never be imagined for legacy grids [2–4]. It also involves consumers for efficient load management e.g., smart grid will use dynamic energy pricing [5]. Thinking rational economically, customers will cut off un-necessary loads at peak demand hours or shift them to low-energy price hours. Smart grids are also expected to integrate large number of small and micro distributed generation systems which can be owned by small enterprises or private individuals [6]. Consumers may use self generated electricity (e.g., solar panels) during high energy price hours and even contribute extra generated electricity to the main grid.

Amongst the most innovative and challenging opportunities brought by the smart grid, there is the design of smart home and building automation that can be deployed in both residential and commercial buildings [7,8]. Such smart systems efficiently control all the appliances e.g., air conditioning, heating, refrigerators, washing machines, TV, computers, etc without requiring any physical presence [2]. However, smart systems require an intelligent device e.g., Home Energy Gateway (HEG) at the consumer sites [9,10]. The concept of HEG has been illustrated in Fig. 1. It can be observed that the HEG communicates with all local appliances as well as with the utility using available wired/wireless technologies. The HEG continuously monitors the state of all appliances and manages/controls them for efficient energy management. However, the functionalities of HEG could be quite broad and it may also provide activity logging or raise alarms/notifications under certain conditions e.g., when energy price changes, load increases beyond

* Corresponding author.
E-mail addresses: rafiullah.khan@qub.ac.uk (R. Khan), sarmad.khan@polito.it (S.U. Khan).

http://dx.doi.org/10.1016/j.jii.2017.07.001
2452-414X/

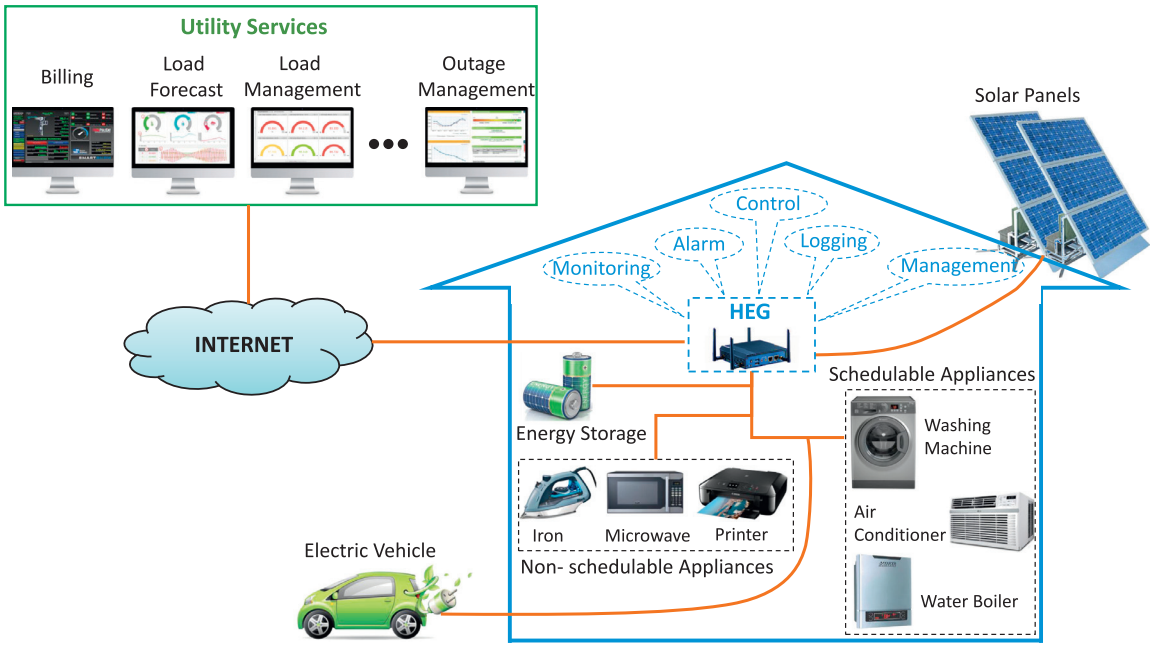


Fig. 1. Demand side management concept.

allowed limit from the utility, etc. The HEG can be configured to control the appliances based on their operational importance, energy price, current load, amount of local generated electricity from solar panels, etc. Note that the HEG could be customized by the local consumers but could also be managed by the utility. It enables the utility to monitor, forecast or manage consumers load. E.g., the utility may set a load threshold and the consumers total load should never exceed that limit. The HEG also enables the utility to remotely control the operational status of schedulable appliances for better load or demand-response management.

The HEG brings the opportunity for rapid development of many smart grid DSM services including but not limited to home/building automation, efficient load management, Advanced Metering Infrastructure (AMI), dynamic energy pricing, distributed power management, etc [9]. A major challenge for the HEG is the design of suitable communication framework that can enable the utility to remotely manage, configure or control plethora of heterogeneous devices at geographically dispersed consumer sites. To this aim, a standardized communication framework should be developed that can address key challenges such as zero-configuration, hassle free seamless discovery and networking, interoperability between plethora of heterogeneous devices from different manufacturers, plug & play feature, privacy and security. Several researchers in literature have developed HEG (or gateway in general) that could address one or more of the key challenges e.g., auto-discovery [9,11], interoperability [10–13], security [14,15], etc. However, the literature still lacks a comprehensive HEG design that could address all key challenges.

The main objective of this paper is to identify key challenges in the design of DSM services and develop a more comprehensive/complete HEG that provides all essential features. Further, the HEG should be configurable and flexible enough to be used for any specific DSM service. To this aim, this paper proposes the design of communication frameworks for the HEG based on Universal Plug & Play (UPnP) [16] and Group Domain of Interpretation (GDOI) [17] enabled secure Hyper Text Transfer Protocol (HTTP). The UPnP enables auto-discovery, zero-configuration and seamless communication between the HEG and plethora of heterogeneous devices at consumer sites. A standard developed service based on UPnP mitigates the interoperability and integration issues between devices from different manufacturers. Whereas, the GDOI enabled secure HTTP protocol is used for communication between the HEG and the utility/electrical grid. The GDOI provides enhanced protection for DSM services against cyber attacks due to its unique and distinguishing feature of periodic security policies and keying material refreshment. This paper provides clear functional specification towards practically implementing the HEG that could support multiple concurrent DSM services. Further, it also functionally evaluates the HEG in real networking environment and presents performance metrics.

The rest of the paper is organized as follows: Section 2 presents background and related work from literature. Section 3 highlights the importance of HEG in the development of different smart grid DSM services. Section 4 presents the design of proposed system and addresses key challenges. Section 5 presents the design of communication frameworks and highlights their unique features. Section 6 presents implementations. Section 7 experimentally evaluates the proposed system. Finally, Section 8 concludes the paper.

2. Background and related work

Efficient demand-response management is a key factor revolutionizing legacy grids into smart grids. Authors in [8] proposed a methodology for estimating power capacity and managing building temperature operation within the DSM system. The system meets demand-response requirements of grid while ensuring quality of service for end-users. Authors in [18] presented a load management service by shifting the operation of deferrable residential loads from peak hours and maximizing the use of power from Photo-Voltaic (PV) units installed on rooftop of homes/buildings. The extra generated electricity from PV units can also be contributed to the main grid. Authors in [19] proposed a system for energy storage optimization under intermittent supply of electricity. The system ensures continuous supply of electricity for critical home appliances by using a predictive scheduling and load management mechanism that reduces discomfort level for the consumers. In short, numerous DSM services will soon become part of the smart grid for better load management [7,20].

Please cite this article as: R. Khan, S.U. Khan, Design and implementation of UPnP-based energy gateway for demand side management in smart grid, Journal of Industrial Information Integration (2017), http://dx.doi.org/10.1016/j.jii.2017.07.001

Although smart grid offers many interesting DSM services, their practical realization is very challenging. Authors in [21] investigated the theoretical and socio-political issues. They have highlighted hurdles from real life experiences, identified need for increased consumer participation in energy management and the need of effective policy making and standards. A major challenge in the realization of DSM services is the communication interface that can enable the utility to remotely manage, configure or control plethora of heterogeneous devices at the geographically dispersed consumer sites. An energy gateway at each consumer site is the most favorable solution identified by several researchers [9,22,23]. The Open Service Gateway initiative (OSGi) alliance initially evolved with main focus on the modular design of gateways [22]. A gateway developed on top of OSGi for Internet of Things (IoT) devices is presented in [24]. It addresses interoperability but lacks to address auto-discovery, plug & play and communication security issues. Authors in [9,25] also focused on the modular design of the HEG for efficient energy management at home. However, [9] uses HTTP client-server mechanism that lacks to address security, interoperability and integration between heterogeneous devices. Whereas, [25] does not focus on the communication aspects. Authors in [26] investigated if the expensive home servers could be replaced with low cost and compact gateways. It was identified that the gateway functionalities are not computing intensive and could be easily supported on low cost Raspberry Pi.

The features and capabilities of the energy gateway also depend on the choice of the communication framework. Several researchers have used MQTT protocol which was originally designed for IoT devices due to its small code footprint and low bandwidth requirement. Authors in [10] presented an MQTT based gateway for home energy management. A cloud-based system collects the home energy consumption and then schedules the operation of home appliances. However, MQTT lacks zero-configuration and seamless discovery features. A similar work using MQTT has also been presented in [12]. Researchers have also used some other IoT protocols for gateway design e.g., CoAP, XMPP, etc. CoAP protocol is specifically designed for constrained devices and has no built-in security mechanism but can operate over DTLS security. Whereas, XMPP is an application profile of the XML and has standard encoding format for messages. This addresses interoperability issues to some extent but it lacks security and seamless auto-discovery features. Gateways designed using CoAP and XMPP are presented in [27] and [13], respectively.

MQTT, CoAP and XMPP are application protocols operating on top of TCP/IP using wired Ethernet or wireless communication. Many researchers have developed gateways using non-TCP/IP based technologies e.g., ZigBee, Bluetooth, etc. Authors in [23,28,29] presented gateways for home energy management using ZigBee wireless technology. Whereas, a gateway using connectionless Bluetooth Low Energy as data communication method has been presented in [30]. It is worth mentioning that ZigBee and Bluetooth are not the best approaches due to compatibility issues, security and limited or no support on legacy gateway devices.

The protocols used in gateway design usually lack a built-in security mechanism. It is essential to ensure communication security using additional security technologies. Communication security within the DSM is a major challenge and several researchers have analyzed different cyber attacks [31–33]. Authors in [34] investigated undetectable or stealthy cyber attacks on AMI service in smart grid and performed the risk assessment. They also identified that a compromised or hacked communication could result in potential theft of electricity. Authors in [35] investigated impact of cyber attacks on energy demand communication from consumers to the utility. To improve communication security, the authors also proposed an Artificial-Noise (AN)-aided encoded mechanism. Authors in [14] proposed a privacy-preserving scheme and presented it for the AMI service. They combined cryptographic primitives such as encryption and identity-committable signatures. Authors in [15] presented a lightweight key establishment mechanism for smart home energy management service. The proposed proof-of-concept provides protection against denial-of-service and eavesdropping attacks.

The energy gateway should also provide zero-configuration and auto-discovery features which are lacking in most gateway designs in literature. Different existing technologies can be used to achieve such features e.g., multicast DNS (mDNS), AllJoyn, IoTivity, UPnP, etc. The mDNS standard is published by Apple Inc. in RFC 6762 [36]. It is used in most Apple products, Google Chromecast, Philips Hue, Spotify Connect and many other devices based on the Avahi software package. However, the mDNS is not a complete communication framework but just service discovery which is its main limitation. After discovery, additional protocols are needed for communication. E.g., authors in [11] combined mDNS discovery with XMPP protocol for IoT devices. Alternatively, AllJoyn, IoTivity and UPnP are complex frameworks which provide seamless discovery and have protocols for communication (command/control) as well. The AllJoyn is an open-source software framework presented by AllSeen Alliance [37]. Due to universal software framework, it enables interoperability between devices supporting AllJoyn. The AllJoyn technology has been adopted by several companies including LG, Panasonic and Sony however, its use in consumer products is still very limited. The IoTivity framework has been developed for constraint IoT devices which have limited processing and memory resources [38]. It uses CoAP and has plugin for MQTT as well. The UPnP technology was originally presented by Open Connectivity Foundation (OCF) [16]. It is a complex communication framework utilizing several different networking protocols to achieve zero-configuration, auto-discovery and seamless communication features. At present, UPnP is the most commonly used technology and is supported on PCs, printers, copiers, Internet gateways, routers, Wi-Fi access points, multimedia streaming systems and even mobile devices. AllJoyn, IoTivity and UPnP have similar goals but the key differences are in their architecture, protocol stack and the way they operate. For example, IoTivity uses CoAP service discovery, AllJoyn uses mDNS service discovery and UPnP uses SSDP protocol for service discovery. IoTivity has notification capability, AllJoyn has publish-subscribe architecture with remote method invocation support and UPnP has notification, remote method invocation and eventing capabilities. UPnP can be the most favorable choice for the design of energy gateway as it is widely adopted/supported on consumer devices, supports eventing as well as command and control features. It supports different state variables each indicating a specific state of the device e.g., ON/OFF, idle/busy, power consumption, etc. Further, it immediately notifies all its peer devices as soon as a state variable changes. It is also worth mentioning that IoTivity, AllSeen Alliance and OCF, all merged together in October 2016. Thus, a unified solution will soon be developed that will combine the best of all technologies and will also be interoperable and backward compatible with current devices using either technology.

Although, several researchers have investigated energy gateway for DSM services, a comprehensive and complete gateway design is still missing. Previous works lack to address at-least one or more of the challenges concerning protocol design, zero-configuration, auto-discovery, seamless plug & play communication, interoperability and integration between plethora of heterogeneous devices, privacy and security issues. Thus, the objective of this paper is to identify all the communication challenges and present the design of a more complete energy gateway that can enable multiple concurrent DSM services. Further, a strong focus is on the communication security and privacy to protect sensitive information from adversaries.

Please cite this article as: R. Khan, S.U. Khan, Design and implementation of UPnP-based energy gateway for demand side management in smart grid, Journal of Industrial Information Integration (2017), http://dx.doi.org/10.1016/j.jii.2017.07.001

3. Importance of home energy gateways

The HEG boosts up the development of new DSM services with the help of its efficient control and management functionalities at the consumer end. It can play a vital role in several evolving DSM services including but not limited to the following:

3.1. Load Management service

The smart grid Load Management (LM) service can balance energy demand with the supply. It enables utility companies to use dynamic energy pricing which helps in preventing unexpected load-shedding/blackouts [5]. Consumers receive energy price from the utility which indirectly represent the current electricity demand at that moment. Utility companies dynamically increase the energy price during peak demand hours to force consumers to reduce their electricity load. Consumers shift their load to low energy price periods in order to reduce their electricity bill. The LM service offers consumers to prioritize their electrical loads and save money by scheduling them to off-peak hours. The HEG plays an important role in the design of LM service by continuously communicating and receiving energy price updates from the utility. A utility normally manages different zones. Each zone usually has different energy requirements during different hours of the day and can have different energy price than other zones. For example industrial zones have high energy demands during day time and bear higher energy price compared to the residential zones. Thus, utility companies will force residential zone and/or industrial zone to reduce the load by increasing the energy price at peak demand hours. Furthermore, this service may grant control of all appliances to the utility who will remotely shutdown the agreed electrical appliances during the critically peak demand hours.

3.2. Home Automation service

The smart grid Home Automation (HA) service helps in reducing energy waste by automating the operational periods of all home appliances. The role of HEG in the design of HA service is vital that activates or deactivates home appliances at pre-specified time. The HEG offers flexibility for consumers to specify configuration for each appliance. The functionalities of the HEG can also be controlled with the help of sensors deployed at different locations at home. Processing the data received from sensors, the HEG decides about the operational state of an appliance at a given time instant. Instead of local appliances control mechanism at the HEG, the control of home appliances may be granted to the utility. The utility will define the use period for different appliances based on their power requirement and operational importance. E.g., a consumer may activate a washing machine which will automatically run during the period specified by the utility. Thus, the utility company may allow high power appliances only to operate at low demand and low energy price periods.

3.3. Advanced Metering Infrastructure service

The Advanced Metering Infrastructure (AMI) service involves two way communication between meters and the utility. The AMI service performs measurements about the electricity consumption, current load, status and diagnostic information from the meters and securely communicates them to the utility. The AMI service relies on the HEG for effectively establishing two-way communication channel for data exchange. The AMI service of the HEG may also receive current energy price and demand-response pattern from the utility and help in efficient integration of renewables and energy storages.

3.4. Distributed Power Generation service

The Distributed Power Generation (DPG) service of the smart grid deals with micro and nano grids. A micro grid is the grouping of electricity generators (e.g., wind farms, solar panels, etc) and consumers over a certain geographical area e.g., a town. It is also capable to operate independently (disconnected from the main grid) by meeting the electricity demand of the local area. Nano grid concept is similar to micro grid but covers a more smaller area e.g., a single building or home. The micro and nano grids may also contribute electricity to the main grid and need the capability to dynamically connect and disconnect from it. It is strictly necessary that micro/nano grid is synchronized (same phase, magnitude and frequency) to the main grid while connecting in order to prevent any physical damage to the equipment. To this aim, time-stamped electrical quantities (known as synchrophasors) are transmitted in real-time to the control center over public Internet. The HEG could play an important role in secure transmission of synchrophasors and dynamic connection/disconnection of micro/nano grids from the main grid. Further, the HEG may also be communicating with the local energy storage devices.

4. Design of proposed system

The design of proposed system is depicted in Fig. 2. It consists of utility, HEG and home appliances. The HEG is communicating with home appliances in the local network while with the utility over the public Internet. Since, two different types of communications are involved, the complexity, challenges and requirements are different. The HEG communication with home appliance in LAN does not face any privacy and security challenges. However, the HEG communication with the utility needs to ensure proper security measures for protection against potential cyber attacks. To this aim, the proposed system in Fig. 2 uses two different types of communication frameworks: UPnP and secure HTTP.

The UPnP communication framework is especially designed for the HEG communication with home appliances. UPnP provides several interesting features including zero-configuration, auto-discovery and seamless networking [16]. After mutual seamless discovery, communicating devices retrieve complete service description of their peer device (i.e., the capabilities of a device). Further, it allows devices to send and receive commands (i.e., control) that result in certain actions performed by the peer device. Actions performed by a UPnP device may result in status change (e.g., power state transition) which is immediately notified to all peer devices (i.e., eventing). The detailed design of UPnP based communication framework is presented in Section 5.1.

The HTTP client/server approach is used for communication between the HEG and utility company. Since, the communication passes over insecure public Internet, the GDOI [17] based security mechanism is proposed as the most effective approach for ensuring integrity and confidentiality. The GDOI provides enhanced security due to periodic refreshment of security credentials [17]. The continuous refreshment of security policies provide best possible protection against cryptanalysis and potential cyber attacks. It can be observed in Fig. 2 that the GDOI is based on Internet Security Association and Key Management Protocol (ISAKMP) for secure authentication between communicating devices over an insecure network. ISAKMP identity protection mechanism consists of three different exchanges: (i) negotiation of security policies between communicating devices (i.e., encryption and signatures algorithms, key size, validity, authentication method, etc), (ii) key establishment mechanism which is based on Diffie Hellman public key cryptography, and (iii) secure authentication using security key established by Diffie Hellman approach. After successful authentication, a new security key is established between the HEG

Please cite this article as: R. Khan, S.U. Khan, Design and implementation of UPnP-based energy gateway for demand side management in smart grid, Journal of Industrial Information Integration (2017), http://dx.doi.org/10.1016/j.jii.2017.07.001

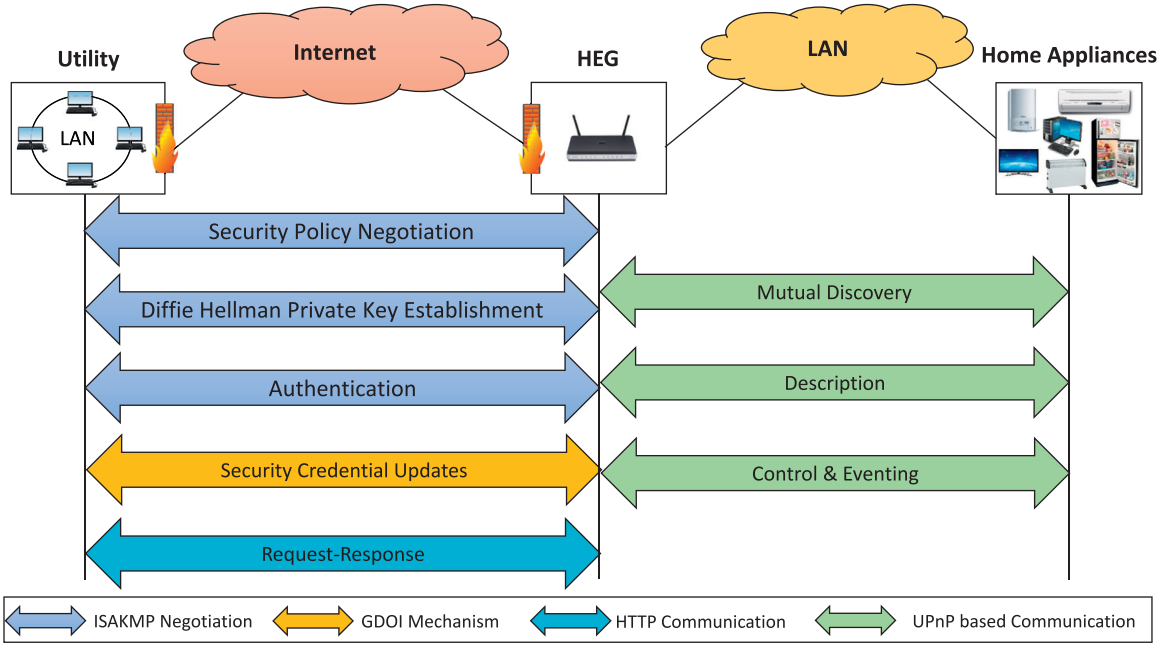


Fig. 2. Overview of proposed system.

and the utility for protecting HTTP based communication. This security key is refreshed periodically based on agreed security policies. In GDOI, key generation and refreshment mechanism can be local (as shown in Fig. 2) or based on an external key distribution center. The detailed design of GDOI based secure HTTP communication framework is presented in Section 5.2.

The basic requirements and design challenges for the proposed system (in Fig. 2) can be classified into three categories: (i) challenges for home appliances, (ii) challenges for the HEG, and (iii) challenges for the utility company.

4.1. Challenges for home appliances

The home appliances need to have the following basic capabilities:

1. Appliances need to have deployment flexibility. They should be able to operate in any network topology (e.g., bus, ring, star, mesh or hybrid).
2. Appliances need to offer interoperability and Integration flexibility. Appliances from different manufacturers need to support common set of features and communicate without any special configurations or specific requirements.
3. For convenience of consumers, appliances should operate as plug and play. They should be able to automatically discover the HEG in the network and seamlessly communicate with it without requiring any network settings from users.
4. Appliances from different manufacturers need to implement a standardized communication framework for easy communication with the HEG. Section 5.1 presents the design of a service based on UPnP framework which can be implemented by any network device.
5. Appliances need to have unique identity as the HEG might be covering a big network and different subnets. Therefore, IP address may not be a good choice, instead Universally Unique IDentifier (UUID) should be used. UUID has a standard format and size (128 bits) and used to uniquely identify a device in the system.
6. Appliances need to know their operational/power state and immediately notify the HEG over suitable communication framework in case of any change. A kernel module can be developed for tracking power state transitions as used in our experimental testbed in Section 7.
7. Appliances need to have a mechanism to update their power state based on the commands received from the HEG. The HEG may instruct a device to transition into a low power sleep/standby state or wakeup from standby state.
8. Appliances need to have a mechanism for remote switching ON or wake-up. Experiments reported in Section 7 were performed assuming a standard PC as an appliance that supports remote wake-up mechanisms known as Wake-On-LAN (WOL) and Wake-on-Wireless-LAN (WoWLAN). Support for such mechanisms could be easily integrated in future home appliances.
9. The home network should be protected from unauthorized access using standard Firewall. Firewall provides protection from intruders for unnecessary switching ON/OFF home appliances.
10. Appliances need to have built-in intelligence and avoid obeying the HEG commands under certain conditions. Under some critical conditions or user need, operation of an appliance may be strictly necessary. Such situations need to be communicated to the HEG to improve its decision making for better energy management at home.

4.2. Challenges for the HEG

The functionalities of the HEG depend on the DSM service. However, it must have the following generic capabilities:

1. It should be always available and easily accessible by the utility and all home appliances at any time.
2. It should be able to communicate with appliances from different manufacturers by implementing a standardized communication framework.
3. It should be able to uniquely identify each appliance based on UUID and keep track of its operational status and capabilities.
4. It should have built-in intelligence that can automate the use of home appliances based on instructions received from the utility.
5. It should support a standardized mechanism for switching ON or waking up an appliance e.g., WOL, WoWLAN, etc.

Please cite this article as: R. Khan, S.U. Khan, Design and implementation of UPnP-based energy gateway for demand side management in smart grid, Journal of Industrial Information Integration (2017), http://dx.doi.org/10.1016/j.jii.2017.07.001

6. It should implement a standardized security mechanism for protecting integrity and confidentiality of communication with the utility.
7. HEG software should have low footprint and easily executable on constraint legacy home gateways with limited memory and processing power.

4.3. Challenges for the utility company

The functionalities of the utility company depend on the type of the DSM service with the following generic capabilities:

1. It should be able to uniquely identify each HEG at different consumer sites and keep track of all appliances and their total instantaneous power consumption.
2. It should implement a standardized security mechanism for ensuring communication security with the HEG.
3. Based on the type of the DSM service, utility will perform different types of functionalities. In general, it should be able to send different commands to the HEG. The HEG will perform certain actions and return the results back to the utility.

5. Design of communication frameworks

It can be observed in Fig. 2 that the HEG communicates with the utility as well as with home appliances. Communication with the utility is remote over the public Internet while with home appliances, it is local. Thus, the proposed system uses two different types of communication frameworks: UPnP for LAN communication and GDOI based secure HTTP for communication over insecure public Internet. This section presents the design of both communication frameworks.

5.1. UPnP based communication framework

The choice of UPnP based communication framework for home network is motivated due to auto-discovery, zero-configuration and seamless networking features [16]. A UPnP device does not require any configuration and automatically connects and communicates with its peer devices. Further, UPnP technology is supported by heterogeneous devices from different manufacturers without causing any interoperability issues. UPnP is a complex architecture that can be customized in variety of ways. This makes UPnP as the most favorable choice for the HEG due to the presence of plethora of different devices from different manufacturers in the home environment. The UPnP technology enables the HEG to automatically discover connected home appliances, monitor their power status and control their operations.

The UPnP architecture is built upon several protocols: (i) Simple Service Discovery Protocol (SSDP) for auto-discovery of network devices, (ii) General Event Notification Architecture (GENA) for notification of status updates, and (iii) Simple Object Access Protocol (SOAP) for sending commands. The SSDP operates on top of HTTPU (an extension of HTTP protocol that uses UDP as transport protocol instead of TCP) whereas SOAP and GENA protocols operate on top of HTTP. GENA also operates on top of HTTP-MU (HTTP using UDP multicast) when the advertisements or notifications are sent to a group of devices.

5.1.1. UPnP device types

The UPnP technology specifies two types of devices: Controlled Device (CD) and Control Point (CP). The role of CP is similar to a client sending instructions/commands which are responded by the specific service of CD.

Fig. 3 depicts the generic structure of a UPnP CP. The Device Manager manages the list of all discovered devices over the network and retrieves their device and service description files. The

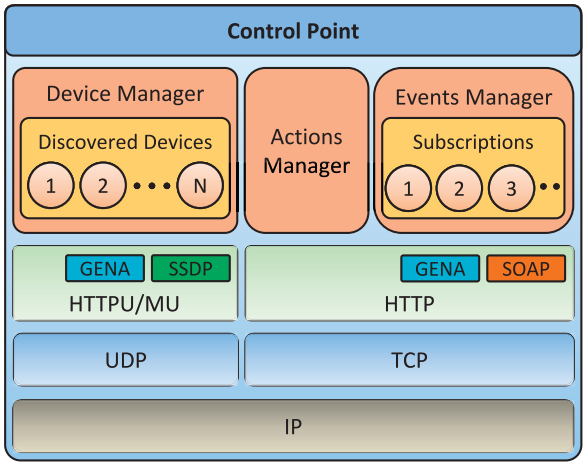


Fig. 3. UPnP Control Point.

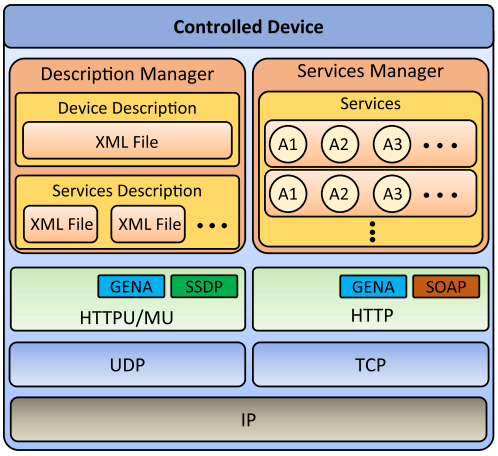


Fig. 4. UPnP Controlled Device.

Action Manager invokes different actions on the CD related to different services. The Event Manager manages different events such as changes in the state variables. It is also responsible to periodically renew the device and service subscriptions before their registration expires. Subscription renewal is particularly important to know about the absence of CD if it accidentally leaves the network due to cable disconnection or any other reason.

Fig. 4 depicts the generic structure of a UPnP CD which is offering one or more services. The Description Manager is responsible for managing the device description as well as the description of all services it is offering. The device and services descriptions are expressed in XML files. The Description Manager is also responsible for periodic advertisement of CD in the network and providing relevant description files. The Services Manager within a CD manages the implementation of different services and their supported actions. The Services Manager receives commands from the CP after which it executes a particular action. It is also responsible to keep the CP updated about the changes in CD status.

5.1.2. Communication paradigm

In the UPnP based communication system, a device either implements a CP or a CD (only one device is capable of sending commands). To achieve two way command and control, both the HEG and home appliances in the proposed system implement a CP as well as a CD as shown in Fig. 5. Fig. 5 also depicts basic communication semantics consisting of the following steps:

Please cite this article as: R. Khan, S.U. Khan, Design and implementation of UPnP-based energy gateway for demand side management in smart grid, Journal of Industrial Information Integration (2017), http://dx.doi.org/10.1016/j.jii.2017.07.001

Table 1
Actions provided by the UPnP power management service offered by home appliances.

Action name	Arguments	Direction	Allowed values	Action description
GetPowerState	UUID	Input	N/A	Provides the HEG its current power state.
	Address	Input	IPv4/IPv6	
	PowerState	Output	ON/OFF/Standby	
	RegID	Output	Integer	
WakeUpMethod	UUID	Input	N/A	Informs the HEG on how to wake it up from standby.
	Address	Input	IPv4/IPv6	
	Method	Output	WOL/WoWLAN	
	RegID	Output	Integer	
OperationOn	UUID	Input	N/A	Appliance starts functioning its job.
	Address	Input	IPv4/IPv6	
	RegID	Output	Integer	
OperationOff	UUID	Input	N/A	Appliance stops functioning its job.
	Address	Input	IPv4/IPv6	
	RegID	Output	Integer	
GoToStandby	UUID	Input	N/A	Appliance goes to standby state.
	Address	Input	IPv4/IPv6	
	RegID	Output	Integer	
StandbyPeriod	UUID	Input	N/A	Appliance will stay in standby state during specified start and stop period.
	Address	Input	IPv4/IPv6	
	StartTime	Input	HH:MM:SS	
	StopTime	Input	HH:MM:SS	
	RegID	Output	Integer	
Withdraw	UUID	Input	N/A	Appliance cancels a specified action previously registered.
	Address	Input	IPv4/IPv6	
	RegID	Input	Integer	

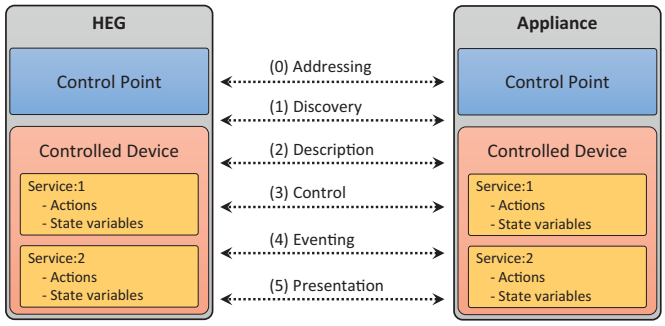


Fig. 5. Proposed UPnP based communication scenario between the HEG and home appliances.

- *Step-0 Addressing:* The home appliance gets an IP address using DHCP (i.e., the HEG also works as gateway device).
- *Step-1 Discovery:* A UPnP device advertises itself and discovers other devices of interest in the network.
- *Step-2 Description:* The CP in each device retrieves CD and service descriptions of its discovered devices.
- *Step-3 Control:* A UPnP device can invoke an action on other UPnP devices.
- *Step-4 Eventing:* A CD updates other UPnP devices about any changes in its operational status.
- *Step-5 Presentation:* A CP retrieves CD information from the presentation URL of the CD.

5.1.3. Description of services

As specified in Section 4, the HEG and home appliances need to implement standardized communication services. Each service implements one or more actions which can be invoked by peer UPnP devices. Table 1 provides the description of UPnP power management service for home appliances. With the knowledge of UPnP service description, the HEG can launch different types of actions on home appliances. The proposed service in Table 1 needs to be implemented by all home appliances. It enables the HEG to launch similar types of actions on all home appliances. The UPnP service also consists of a set of state variables. State variables represent the current state of the device/appliance. Table 1 also lists the state variables for home appliances (i.e., PowerState, Method, StartTime, StopTime, etc).

Similarly, the HEG needs to implement a standardized service to achieve interoperability and zero-configuration with home appliances. Table 2 provides the description of proposed UPnP service offered by the HEG. It offers similar types of actions invokable by all home appliances.

5.2. GDOI based secure HTTP communication framework

The GDOI based secure HTTP communication framework is used for communication between the HEG and the utility. Since the communication takes place over the public Internet, the information security becomes crucial. It is likely possible that the HEGs may be manufactured by different vendors. A generalized and standardized communication framework is necessary to achieve ease of integration and interoperability. The HTTP can be the most suitable choice as communication protocol due to its structured meta-data and non-restricted flow through Firewalls (at-least in outgoing direction). However, the HTTP protocol itself is insecure and vulnerable for cyber attacks targeting integrity and confidentiality of communication.

The proposed system in Fig. 2 is a group-based system where multiple HEGs will be communicating with a single utility company. Thus, the utility is coordinating with a group of HEGs and requires an efficient group-based security mechanism. The GDOI emerged as a most successful group-based security mechanism [17]. Key features of the proposed security mechanism include: (i) secure key establishment over public Internet using Diffie Hellman approach, (ii) protection against spoofing by the use of cryptographic signature inside packets, (iii) encryption of packets based on multiple supported algorithms for achieving high level of confidentiality and protection against integrity attacks, (iv) periodic update of security policies and keying material to achieve maximum possible protection against cryptanalysis, and (v) easily customizable for real-time communication and supported by plethora of heterogeneous devices using any specific protocol. These unique qualities make the GDOI a suitable security framework for protecting communication between the HEGs and the utility.

Please cite this article as: R. Khan, S.U. Khan, Design and implementation of UPnP-based energy gateway for demand side management in smart grid, Journal of Industrial Information Integration (2017), http://dx.doi.org/10.1016/j.jii.2017.07.001

Table 2
Actions provided by the UPnP service offered by the HEG.

Action name	Arguments	Direction	Allowed values	Action description
WakeUpTime	UUID	Input	N/A	The HEG will wake up the appliance at specified time.
	Address	Input	IPv4/IPv6	
	Time	Input	HH:MM:SS	
	RegID	Output	Integer	
NoStandbyPeriod	UUID	Input	N/A	The HEG will never put the appliance into standby state during the specified start and stop period.
	Address	Input	IPv4/IPv6	
	StartTime	Input	HH:MM:SS	
	StopTime	Input	HH:MM:SS	
	RegID	Output	Integer	
Withdraw	UUID	Input	N/A	The HEG cancels a specified action previously registered.
	Address	Input	IPv4/IPv6	
	RegID	Input	Integer	

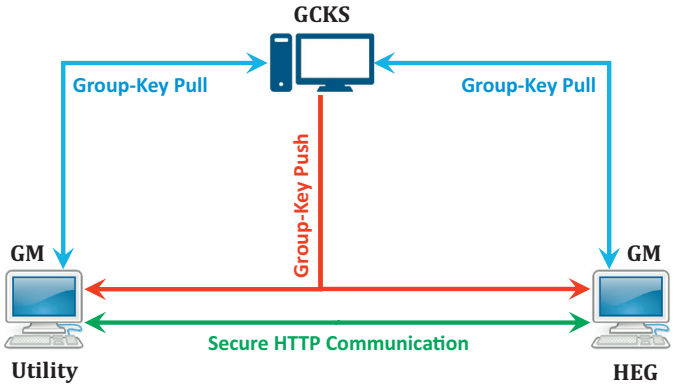


Fig. 6. Proposed GDOI-based secure HTTP communication framework.

The GDOI security model consists of two types of devices: Group Controller and Key Server (GCKS) and Group Members (GM). GCKS is responsible for providing security policies (e.g., signature algorithm, encryption algorithm, key life type, key length, key validity, authentication method, etc) and keying material to group members. The group members then utilizes acquired security credentials for secure communication among one another and with GCKS. In the proposed system in Fig. 2, the utility plays the role of GCKS as well as a group member. Whereas, the HEGs function as group members. The GDOI mechanism utilizes three types of keys:

1. Pair-wise Key: Pair-wise key is either pre-distributed or secretly established using any public key cryptography mechanism. This paper reports implementations based on Diffie Hellman mechanism which enables the HEG and the utility to establish a secret key over the public Internet.
2. Key Encryption Key (KEK): After successful authentication and pair-wise key establishment, GCKS provides KEK and its associated security policies to the HEG. The acquired security policies and keying material is then used to protect any future communication in which GCKS provides key or security policies updates to the HEG.
3. Traffic Encryption Key (TEK): The KEK is used for encryption of messages in which the utility provides TEK to the HEGs. The TEK is then used to encrypt/decrypt two-way messages exchanged over HTTP between the utility and the HEG.

The proposed GDOI-based secure communication framework is depicted in Fig. 6. The GCKS is internal part of the utility in the proposed system but depicted as separate standalone entity in Fig. 6 for the sake of clarity. The security mechanism consists of two phases:

- Phase 1: This phase is known as authentication and pair-wise key establishment phase using Internet Security Association and Key Management Protocol (ISAKMP). The HEG and the utility send a request to GCKS for security policies related to KEK and TEK (known as Group-Key-Pull). The acquired security policies are then used for communication between the HEG and the utility.
- Phase 2: This phase is known as Group-Key-Push. It is worth to mention that both KEK and TEK in the GDOI mechanism have certain validity and must be replaced periodically. GCKS uses Group-Key-Push messages to provide KEK and TEK to the HEG and the utility before the expiry of current security credentials.

6. Implementations

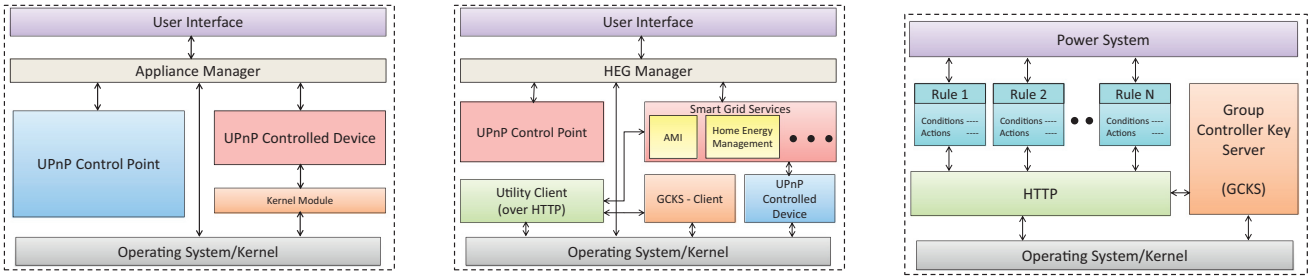
The proposed system consists of three software entities: (i) home appliance, (ii) HEG and (iii) utility. The basic structure of each software entity is shown in Fig. 7. Note that home appliances and the HEG communicate using UPnP technology whereas the utility and the HEG communicate over HTTP. All software entities were developed in Linux OS using standard C/C++ programming language with the help of libupnp libraries and boost libraries.

6.1. Home appliance software

Fig. 7(a) depicts the basic components of software for home appliances. It implements both UPnP CP as well as CD. For sake of simplicity, it does not show the functional blocks of CP and CD which could be referenced in Figs. 3 and 4, respectively. UPnP CP and CD implement all the functionalities reported in Section 5.1. The CP is used to instruct the HEG with different conditions (e.g., only run this appliance when energy price is below certain threshold or operation of this appliance is crucial and should not be stopped under any condition for DSM load management service, etc). The CD receives commands from the HEG to control the operational status of the appliance (e.g., put appliance into sleep state, stop or resume the operations of the appliance, etc).

The home appliance software provides all the basic functionalities reported in Section 4.1. The use of UPnP technology provides plug & play features and deployment flexibility. The CP and CD use SSDP protocol for discovery which enables the HEG to seamlessly discover the home appliances as soon as they are connected to the network. The interoperability and integration issues (between devices from different manufacturers) are addressed through the design of a service with common set of features. At present, the CD in home appliance software implements the service described in Table 1. The implementation of this service by all home appliances enables the HEG to execute similar actions on them. The UPnP CD (see Fig. 4) also includes device/appliance and its service descriptions which are saved in the XML files. During discovery, the HEG downloads the device/appliance XML description that also includes a UUID. The HEG uniquely identify an appliance based on its UUID.

Please cite this article as: R. Khan, S.U. Khan, Design and implementation of UPnP-based energy gateway for demand side management in smart grid, Journal of Industrial Information Integration (2017), http://dx.doi.org/10.1016/j.jii.2017.07.001



(a) Appliance (b) HEG (c) Utility

Fig. 7. Basic software structures in the proposed system.

Note that the CD service description consists of a list of state variables each indicating a specific operational state of the device (e.g., busy, idle, power state, sleep periods, etc). As soon as a state variable value changes, the UPnP CD immediately notifies the HEG. The software for home appliances also implements a kernel module which tracks the operational status e.g., ON, OFF, low power sleep, etc. Whenever the appliance operational state changes, kernel module immediately notifies the CD which eventually notifies the HEG. Based on the state variables, the home appliance software may deny executing a certain action requested by the HEG (e.g., appliance is busy and the HEG requested it to turn OFF or go to sleep state). Since, software is executed on Linux OS, its built-in system calls are used to change the power state of the appliance. When the HEG wants to wake-up an appliance, it uses the WOL mechanism which is supported by most modern Network Interface Cards (NICs).

6.2. HEG software

Fig. 7(b) depicts simplified structure of the HEG software. Likewise home appliances, it also implements both UPnP CP (functional blocks in Fig. 3) as well as CD (functional blocks in Fig. 4) for enabling two way command and control features. The CP is used for controlling the operational status of home appliances. While CD receives instructions from home appliances e.g., when to operate an appliance in case of dynamic energy pricing. The Utility Client communicates with the utility over HTTP protocol. It enables the utility to communicate with local implementation of the DSM services e.g., retrieving current meter reading, reducing load in home, etc. The GCKS client communicates with the GCKS to acquire security credentials which are used to protect HTTP communication between the HEG and the utility. Further, it is responsible to keep security credentials up-to-date by periodically receiving them from the GCKS. Current implementations support AES-128-GCM, AES-256-GCM and AES-256-CBC as encryption algorithms. The supported signature algorithms include: HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512 and AES-GMAC-128.

The HEG software provides all the basic functionalities reported in Section 4.2. Since, the HEG and home appliances are using UPnP technology, they seamlessly discover and communicate with each other without facing any interoperability issues. At present, the CD of the HEG software implements the service described in Table 2. It enables all home appliances to send similar commands to the HEG. Note that the HEG software also implements WOL technology i.e., remote network-based trigger of home appliances. The HEG accomplishes this by broadcasting a specific message (also known as magic packet) in the local network. The magic packet contains in its payload 6 Bytes of all 255 (FF FF FF FF FF FF in hexadecimal) followed by the 48-bit MAC address of the sleeping appliance repeated 16 times (total payload size 102 Bytes). When the NIC of the appliance detects WOL packet, it immediately triggers the power-up interrupt line on the motherboard and the appliance becomes fully operational again.

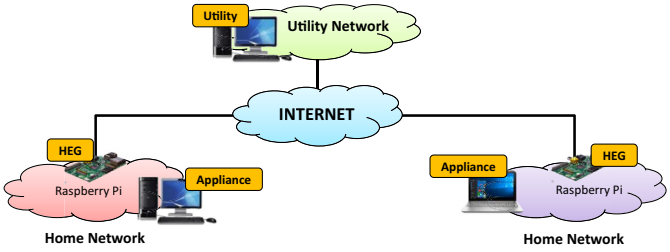


Fig. 8. Experimental testbed.

6.3. Utility software

To be quite generic for any type of smart grid DSM service, Fig. 7(c) depicts the basic structure of the utility software. Power System block is service-specific. It is providing different power system credentials to the behavioral Rules e.g., energy price (if the proposed system is implementing dynamic energy pricing), demand and supply information (i.e., load management service), etc. Each Rule implements a specific DSM service e.g., AMI, load management, home automation, etc. It invokes certain actions based on conditions met on the data supplied by Power System block. The utility software also implements HTTP client and server for communication and invoking actions on the HEG. The HTTP communication security is ensured using the GDOI security mechanism. The HTTP block is communicating with GCKS to determine which security policies and keying material to use to protect the HTTP communication. The GCKS implements all of the operations discussed in Section 5.2. It is worth to mention that GCKS does not operate over HTTP but communicates with GCKS-client on the HEG using standard UDP protocol.

7. Evaluation of proposed system

Fig. 8 depicts the experimental testbed used for the evaluation of proposed system. It consists of a utility company which is communication with the HEG at different homes. The HEG software is expected to be executed on legacy gateway devices. However, due to no availability of development gateway kit, it has been executed on a very low power device i.e., Raspberry Pi v2 (ARMv6 CPU 700 MHz, 512 MB memory and 3.8 W full load power consumption) for experimental purpose. In future, home appliances such as TV, refrigerators, heaters, boilers, air conditioning and lightening system will also become part of the home network. However, a standard desktop PC was assumed as basic home appliance in Fig. 8 just for the sake of experiments.

Please cite this article as: R. Khan, S.U. Khan, Design and implementation of UPnP-based energy gateway for demand side management in smart grid, Journal of Industrial Information Integration (2017), http://dx.doi.org/10.1016/j.jii.2017.07.001

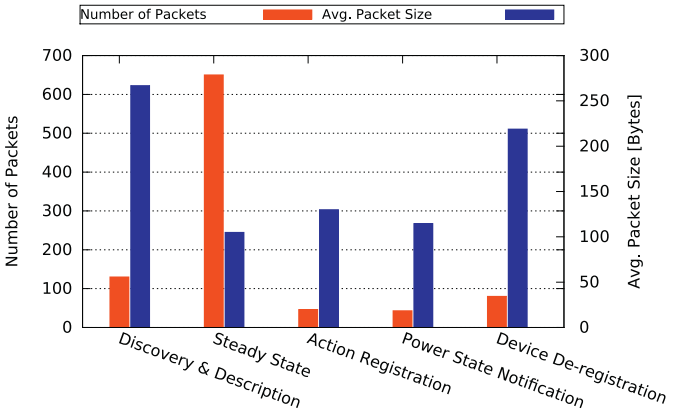


Fig. 9. Number of packets exchanged and the average packet size during different UPnP events.

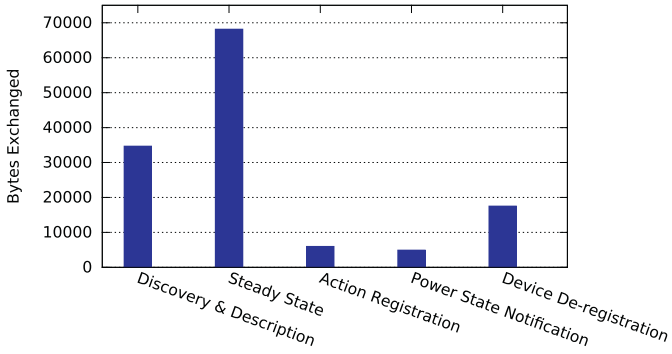


Fig. 10. Total Bytes exchanged during different UPnP events.

The first step of evaluation is to check if all the software entities functionally behave correctly. The practical demonstrations in testbed verified the correct functioning of the utility, the HEG and home appliances. The HEG was able to successfully discover home appliances (i.e., PCs) in transparent and seamless manner without any configurations hassle due to the unique features of UPnP. This highlights the importance of UPnP in proposed system to achieve interoperability and integration between appliances from different manufacturers. The HEG was able to promptly discover and communicate with the home appliances as soon as they connect to the network. All UPnP control and command functionalities reported in Tables 1 and 2 were successfully tested along with the functionalities of the kernel module. The kernel module successfully tracked the operational status of home appliances and immediately notified the HEG in case of updates. The HEG was able to control the home appliances using built-in system calls available on any Operating System (although tests were performed on Linux OS). These system calls then in turn changes the operational/power state of the home appliances. The HEG was also able to wake up home appliances from low-power sleep states by sending WOL packets. The functionalities of GDOI based security mechanism (reported in Section 5.2) were also successfully verified that protected the HTTP communication between the HEG and the utility.

The next step of evaluation is the measurement and assessment of different performance metrics. The following subsections present the measurement of different performance critical factors such as communication overhead, memory requirement, bandwidth requirement, communication latencies, etc. Further, security strength of the GDOI mechanism has also been analyzed.

7.1. Communication overhead

Communication overhead is considered as one of the important performance factor for any protocol. Indirectly, it represents the maximum size of data that can be carried by a single packet. Further, communication overhead is also linked with bandwidth requirement. A protocol with high overhead will potentially operate slower on low bandwidth links.

We performed the overhead analysis for different UPnP events including discovery, device and action registration, state variable updates and device de-registration. The test were performed over the period of 12 min during which the home appliance registers with the HEG, the HEG invokes a control action on the appliance by putting it into sleep state, the HEG wakes up again the appliance using WOL mechanism and finally the appliance de-registers with the HEG. Fig. 9 depicts the number of packets exchanged and the average packet size during different UPnP events. It can be observed that large number of packets were exchanged during the steady-state condition. However, most of the packets exchanged under steady-state condition are for periodic presence advertisement. Such packets are very small in size. The discovery and description packets are very large in size. It is due to the fact that both the HEG and home appliance download complete UPnP service descriptions of each other. Power state notifications are very infrequent and are transmitted only when power state of the home appliance changes. The total Bytes exchanged during different UPnP events are analyzed in Fig. 10. It shows that most Bytes are exchanged during appliance discovery/registration and steady state. For the sake of clarity, Fig. 11 depicts percentage distribution of packets during different UPnP events.

In Fig. 12, we classified the overhead into real information inside packets, overhead due to UPnP formatting of real data, overhead due to UPnP formatting and packet header and total overhead due to UPnP semantics. Fig. 12 also depicts that the packets are quite large in device registration and de-registration phases. It is due to the fact that both, HEG and home appliance download complete CD and service descriptions expressed in the XML format. The overhead analysis confirmed that the large size packets are quite infrequent while the frequently exchanged packets under steady state condition are very small in size. Although, each packet consists of more than 80% overhead Bytes, but it does not affect the system reliability when the frequently exchanged packets are very small in size.

7.2. Resource requirements

This section analyzes the required resources for proposed system in terms of memory and bandwidth requirement. For smooth and reliable operations, minimum required resources must be available. Devices running the utility and home appliance software packages might be equipped with enough memory. However, legacy gateway devices are equipped with low memory (typically 8MB, 16MB or 32MB). To this aim, we also analyzed the memory requirement for the HEG software in Table 3. The HEG software requires 5.12MB of memory due to the implementation of complex UPnP technology and GDOI security mechanism. However, the memory requirement is still lower than the available memory on legacy gateway devices.

Table 3 also presents bandwidth requirement for both, UPnP and GDOI based HTTP communication frameworks. Bandwidth is the most critical factor for any protocol. Protocols with high overhead and high data transmission rates can cause traffic congestion on low bandwidth links or even the packet loss. It can be observed in Table 3 that the bandwidth requirement is significantly low compared to available technologies today (Gigabit Ethernet: 1 Gbps, wireless 802.11b: 11 Mbps, wireless 802.11n: 600 Mbps, ADSL lite: 1.5 Mbps, ADSL2+: 24 Mbps, etc). UPnP has high com-

Please cite this article as: R. Khan, S.U. Khan, Design and implementation of UPnP-based energy gateway for demand side management in smart grid, Journal of Industrial Information Integration (2017), http://dx.doi.org/10.1016/j.jii.2017.07.001

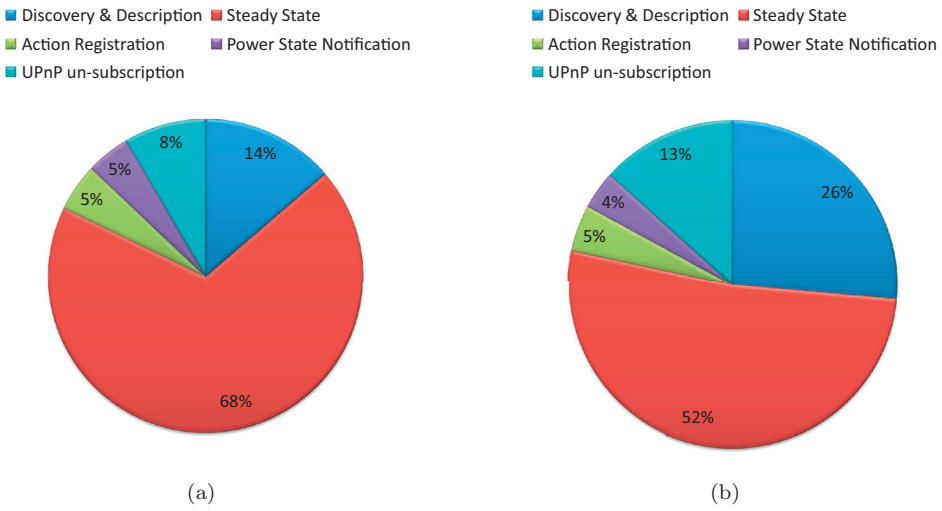


Fig. 11. UPnP overhead analysis: (a) Percentage of total packets exchanged during different UPnP events, (b) Percentage of total Bytes exchanged during different UPnP events.

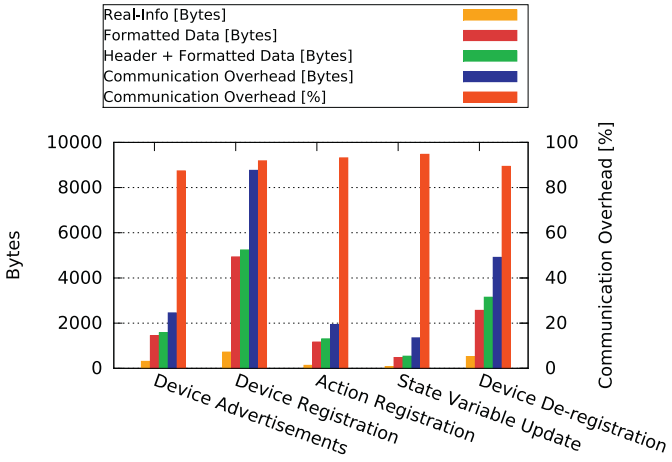


Fig. 12. UPnP overhead analysis in the proposed system.

Table 3
Latency analysis and resource requirements.

Memory requirements		
Utility Software 3.07MB	HEG Software 5.12MB	Appliance Software 4.53MB
Communication Latency Analysis		
UPnP Communication 96.33 ms		HTTP Communication 1.29 s
Bandwidth Requirements		
UPnP Communication 1.48 kbps		HTTP Communication 0.37 kbps

munication overhead but still has very low bandwidth requirement. This is due to low packet transmission rates in UPnP.

7.3. Communication latencies

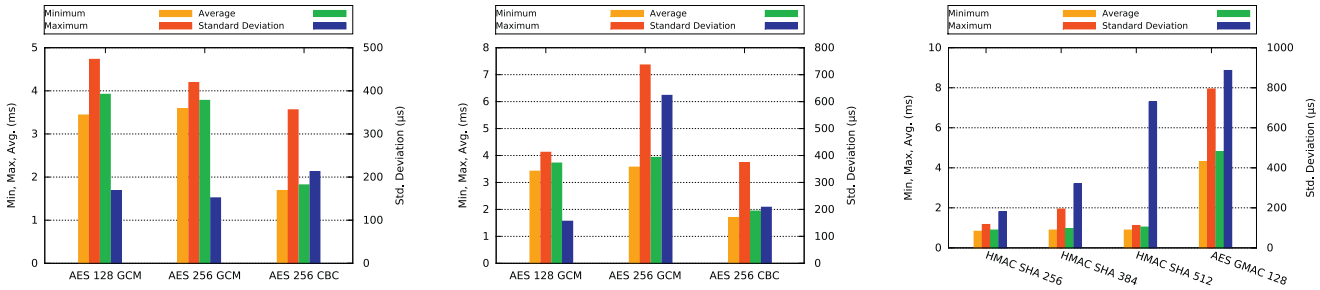
Communication latencies can severely impair the performance of time-critical applications. Low latencies are critically important in our proposed system as long HTTP communication delays may prevent the HEG from receiving updates on security policies and keying material before the expiry of previous security credentials. Long UPnP communication delays may prevent transmission of power state notifications from home appliances to the HEG (such notifications must be transferred in shortest possible time before the appliance actually enters into sleep/OFF state).

Table 3 presents communication latencies for both, UPnP and HTTP communication frameworks. The reported latencies take into account software processing latency (i.e., encoding/decoding of packets) as well as network latency (i.e., packet latency to traverse the network). The network latency depends on the available bandwidth and could be high on low bandwidth channels. Whereas, software processing latency depends on the processing power of the device (i.e., Raspberry Pi in our experiments). The latencies of encryption and signatures algorithms also impact the software processing latency. Fig. 13 presents minimum, maximum, average and standard deviation of processing latencies observed for different types of supported encryption and signature algorithms over 100 trials. It can be observed that processing latencies depend on the type of algorithm used. However, the average value is always less than 10 ms. Due to very low processing latencies, the functionalities of developed software entities are not negatively affected. The UPnP communication latency between the HEG and home appliances is very low (see Table 3). When the kernel receives power state transition request, appliance normally takes 1–2 s for freezing operations and entering into sleep/OFF state. Due to very low UPnP communication and processing latencies, the home appliances (i.e., PCs in our experiments) can successfully notify their power state transitions to the HEG just before the power state transitions actually take place. The reported HTTP communication latency in Table 3 between the HEG and utility is a bit high. A significant portion of this latency is contributed by NO-IP dynamic DNS service used in our experiments. The HTTP communication latency will be very small if the third-party DNS service is not used. However, GCKS provides updates on security policies and keying material to HEGs 5 s before the expiry of previous security credentials in current implementations. Due to such safety margin, HTTP communication latency does not negatively impact the functionalities of the utility and the HEG.

7.4. Security analysis

This section analyzes the importance of security mechanism for HTTP based communication between the utility and the HEG. Since, HTTP does not have a built-in security mechanism, it is vulnerable for different types of cyber attacks. These attacks may impair the communication, cause financial loss to the utility and con-

Please cite this article as: R. Khan, S.U. Khan, Design and implementation of UPnP-based energy gateway for demand side management in smart grid, Journal of Industrial Information Integration (2017), http://dx.doi.org/10.1016/j.jii.2017.07.001



(a) Encryption Latencies (b) Decryption Latencies (c) Signature Latencies

Fig. 13. Observed latencies for supported algorithms averaged over 100 packets.

sumers or may cause physical damage to equipment depending on the DSM service under consideration. This paper analyzes vulnerabilities based on well known CIA (Confidentiality, Integrity, Availability) model. The HTTP protocol in its standard form offers no confidentiality, no integrity and availability that can be easily targeted. Further, it is highly vulnerable to reconnaissance attacks. The unauthorized learning in reconnaissance enables the attacker to launch more sophisticated attacks such as authentication/access, Man In The Middle (MITM), replay/reflection and Denial of Service (DoS). Authentication or access attack provides an adversary the unauthorized access to the HEG or the utility. After successful attack, the adversary may execute unnecessary actions with the objective of stealing information, causing financial loss or damage to physical equipment. The attacker in MITM attack can hijack and modify packets between the HEG and the utility and force them to perform unintentionally misleading decisions. Replay or reflection attack is somehow similar to MITM but instead of modifying packets, it records the communication between the HEG and the utility. The recorded packets are later played back to deceive the HEG or the utility with out-dated packets. An adversary may also launch DoS attack by flooding the HEG or the utility with high data rate packets to exhaust available resources (e.g., memory, bandwidth, CPU, etc) and make it non-responsive.

The GDOI security mechanism can provide strong protection for HTTP communication against different types of attacks. It provides protection against reconnaissance/eavesdropping through encryption. Authentication or access attacks could be easily prevented as the adversary or unauthorized device cannot retrieve security policies and keying material from GCKS. Without the knowledge of keying material (KEK, TEK) and security policies (e.g., encryption algorithm, authentication algorithm, signature algorithm, key validity, etc), MITM attacks could not be executed. The periodic security policies and keying material update feature of the GDOI provides protection against cryptanalysis as well as replay attacks. The HEG or the utility can easily identify replayed packets as the old recorded packets will be based on expired security policies. The GDOI also significantly reduces the strength of DoS attack by using cookies inside each packet. Based on cookies, the GDOI can easily identify DoS packets and simply discard them without processing to save CPU and memory resources. Even though, its not the absolute protection against DoS attack, but the impact of DoS attack is significantly reduced. Table 4 summarizes the effectiveness of GDOI security mechanism against different types of cyber attacks.

Table 4
Security analysis of HTTP-based communication between the utility and the HEG.

		Without GDOI	With GDOI
CIA Model	Confidentiality	None	Strong
	Integrity	None	Strong
	Availability	Vulnerable	Vulnerable
Attack Type	Reconnaissance	Vulnerable	Protected
	Authentication/Access	Vulnerable	Protected
	Man In The Middle (MITM)	Vulnerable	Protected
	Replay / Reflection	Vulnerable	Protected
	Denial of Service (DoS)	Vulnerable	Vulnerable

8. Conclusion

The integration of ICT in smart grid provides enormous opportunities for efficient management and utilization of electricity at the demand side. The concept of HEG has recently been proposed in literature that enables rapid prototyping of new DSM services which could never be imagined before. However, literature still lacks a comprehensive HEG that is equipped with all essential features such as zero-configuration, hassle free seamless discovery and networking, interoperability between plethora of heterogeneous devices/appliances from different manufacturers, customers privacy and communication security.

This paper presented a more complete design of the HEG that can easily integrate multiple concurrent DSM services. In particular, it identified key challenges in the design of DSM services and proposed solution using the HEG equipped with UPnP and GDOI based secure HTTP communication frameworks. The paper identified that UPnP is the ideal choice for communication between the HEG and home appliances. A standard service developed based on UPnP can provide auto-discovery and seamless plug & play communication features. Further, UPnP also addresses interoperability and integration issues between the HEG and plethora of home appliances. This paper evaluated the effectiveness of UPnP communication framework based on experiments performed in real networking environment.

To ensure communication security between the HEG and the utility, this paper also presented the design of an effective GDOI-based security mechanism. It has been analyzed that the GDOI has several distinguishing features which provide best possible protection against eavesdropping, reconnaissance, connection hijacking, authentication/access attack, replay/reflection attack, man in the middle and DoS attacks. The periodic security policies and keying material refreshment makes the GDOI a very strong security mechanism against cyber attacks. Thus, the GDOI can be a well suited security mechanism for the design of emerging DSM services.

References

[1] J.-S. Chou, N.-T. Ngo, Smart grid data analytics framework for increasing energy savings in residential buildings, in: Elsevier Journal of Automation and Construction, 72, 2016, pp. 247–257.
[2] M. Shakeri, M. Shayestegan, H. Abunima, S.S. Reza, M. Akhtaruzzaman, A. Alamoud, K. Sopian, N. Amin, An intelligent system architecture in home energy management systems (HEMS) for efficient demand response in smart grid, in: Elsevier Journal on Energy and Buildings, 138, 2017, pp. 154–164.

Please cite this article as: R. Khan, S.U. Khan, Design and implementation of UPnP-based energy gateway for demand side management in smart grid, Journal of Industrial Information Integration (2017), http://dx.doi.org/10.1016/j.jii.2017.07.001

[3] A.R. Khan, A. Mahmood, A. Safdar, Z.A. Khan, N.A. Khan, Load forecasting, dynamic pricing and dsm in smart grid: a review, in: Elsevier Journal on Renewable and Sustainable Energy Reviews, 54, 2016, pp. 1311–1322.
[4] M.H. Yaghmaee, M.S. Kouhi, A.L. Garcia, Personalized pricing: a new approach for dynamic pricing in the smart grid, IEEE Smart Energy Grid Engineering (SEGE), 2016.
[5] Q. Tang, K. Yang, D. Zhou, Y. Luo, F. Yu, A real-time dynamic pricing algorithm for smart grid with unstable energy providers and malicious users, in: IEEE Internet of Things Journal, 3, 2016, pp. 554–562.
[6] M.L. Tuballa, M.L. Abundo, A review of the development of smart grid technologies, in: Elsevier Journal on Renewable and Sustainable Energy Reviews, 59, 2016, pp. 710–725.
[7] B. Zhou, W. Li, K.W. Chan, Y. Cao, Y. Kuang, X. Liu, X. Wang, Smart home energy management systems: concept, configurations, and scheduling strategies, in: Elsevier Joural on Renewable and Sustainable Energy Reviews, 61, 2016, pp. 30–40.
[8] J.A. Gomez, M.F. Anjos, Power capacity profile estimation for building heating and cooling in demand-side management, in: Elsevier Journal on Applied Energy, 191, 2017, pp. 492–501.
[9] R. Bolla, M. Giribaldi, R. Khan, M. Repetto, Design of home energy gateway boosting the development of smart grid applications at home, in: 2013 4th Annual International Conference on Energy Aware Computing Systems and Applications (ICEAC), 2013.
[10] C.H. Lee, Y.H. Lai, Design and implementation of a universal smart energy management gateway based on the internet of things platform, in: IEEE International Conference on Consumer Electronics (ICCE), 2016.
[11] R. Klauck, Seamless integration of smart objects into the internet using XMPP and mDNS/DNS-SD, PhD Dissertation, Brandenburg University of Technology Cottbus-Senftenberg, Germany, 2016.
[12] Y. Upadhyay, A. Borole, D. Dileepan, MQTT based secured home automation system, Symposium on Colossal Data Analysis and Networking (CDAN), 2016.
[13] S.K. Viswanath, C. Yuen, W. Tushar, W.T. Li, C.K. Wen, K. Hu, C. Chen, X. Liu, System design of the internet of things for residential smart grid, in: IEEE Wireless Communications Journal, 23, 2016, pp. 90–98.
[14] Y. Gong, Y. Cai, Y. Guo, Y. Fang, A privacy-preserving scheme for incentive-based demand response in the smart grid, in: IEEE Transactions on Smart Grid, 7, 2016, pp. 1304–1313.
[15] P. Kumar, A. Gurtov, J. Iinatti, M. Ylianttila, M. Sain, Lightweight and secure session-key establishment scheme in smart home environments, in: IEEE Sensors Journal, 16, 2016, pp. 254–264.
[16] Open Connectivity Foundation. Available at: https://openconnectivity.org.
[17] B. Weis, S. Rowles, T. Hardjono, The group domain of interpretation (GDOI), Internet Engineering Task Force (IETF) Request For Comments (RFC): 6407, Oct. 2011.
[18] E. Yao, P. Samadi, V.W.S. Wong, R. Schober, Residential demand side management under high penetration of rooftop photovoltaic units, in: IEEE Transactions on Smart Grid, 7, 2016, pp. 1597–1608.
[19] J. Khoury, R. Mbayed, G. Salloum, E. Monmasson, Predictive demand side management of a residential house under intermittent primary energy source conditions, in: Elsevier Journal on Energy and Buildings, 112, 2016, pp. 110–120.
[20] S.J. Lee, H. Yang, J.S. Kim, S.G. Choi, Supply and demand management system based on consumption pattern analysis and tariff for cost minimization, in: 18th International Conference on Advanced Communication Technology (ICACT), 2016.
[21] A. Mengolini, F. Gangale, J. Vasiljevska, Exploring community-oriented approaches in demand side management projects in Europe, MDPI Journal on Sustainability, 8, 2016.
[22] OSGi Alliance. Available at: https://www.osgi.org.
[23] Z. Zhao, K. Agbossou, A. Cardenas, Connectivity for home energy management applications, in: IEEE PES Asia-Pacific Power and Energy Engineering Conference (APPEEC), 2016.
[24] N. Verba, K.-M. Chao, A. James, D. Goldsmith, X. Fei, S.-D. Stan, Platform as a service gateway for the fog of things, Elsevier Journal on Advanced Engineering Informatics, 2016.
[25] F. Ding, A. Song, E. Tong, J. Li, A smart gateway architecture for improving efficiency of home network applications, Journal of Sensors, 2016.
[26] A. Grguric, M. Mosmondor, D. Huljenic, Development of low cost energy efficient home sensing internet gateway: a pilot study, in: IEEE International Black Sea Conference on Communications and Networking (BlackSeaCom), 2016.
[27] C. Pham, Y. Lim, Y. Tan, Management architecture for heterogeneous iot devices in home network, in: IEEE 5th Global Conference on Consumer Electronics, 2016.
[28] X.J. Yi, M. Zhou, J. Liu, Design of smart home control system by internet of things based on ZigBee, in: IEEE 11th Conference on Industrial Electronics and Applications (ICIEA), 2016.
[29] C. Peng, J. Huang, A home energy monitoring and control system based on ZigBee technology, in: International Journal on Green Energy, 13, 2016, pp. 1615–1623.
[30] M. Choi, J. Han, I. Lee, An efficient energy monitoring method based on bluetooth low energy, in: IEEE International Conference on Consumer Electronics (ICCE), 2016.
[31] G. Liang, J. Zhao, F. Luo, S. Weller, Z.Y. Dong, A review of false data injection attacks against modern power systems, IEEE Transactions on Smart Grid, 2017.
[32] I. Colak, S. Sagiroglu, G. Fulli, M. Yesilbudak, C.-F. Covrig, A survey on the critical issues in smart grid technologies, in: Elsevier Journal on Renewable and Sustainable Energy Reviews, 54, 2016, pp. 396–405.
[33] R. Khan, P. Maynard, K. McLaughlin, D. Laverty, S. Sezer, Threat analysis of blackenergy malware for synchrophasor based real-time control and monitoring in smart grid, in: Proceedings of the 4th International Symposium for ICS & SCADA Cyber Security Research, 2016.
[34] J. Yao, P. Venkitasubramaniam, S. Kishore, L.V. Snyder, R.S. Blum, Network topology risk assessment of stealthy cyber attacks on advanced metering infrastructure networks, in: 51st Annual Conference on Information Sciences and Systems (CISS), 2017.
[35] A.E. Shafie, D. Niyato, R. Hamila, N. Al-Dhahir, Impact of the wireless network's PHY security and reliability on demand-side management cost in the smart grid, in: IEEE Access Journal, 5, 2017, pp. 5678–5689.
[36] S. Cheshire, M. Krochmal, Multicast DNS (mDNS), in: Internet Engineering Task Force (IETF) Request For Comments (RFC): 6762, 2013.
[37] AllSeen Alliance. Available at: https://allseenalliance.org.
[38] IoTivity. Available at: https://www.iotivity.org.

Please cite this article as: R. Khan, S.U. Khan, Design and implementation of UPnP-based energy gateway for demand side management in smart grid, Journal of Industrial Information Integration (2017), http://dx.doi.org/10.1016/j.jii.2017.07.001

Rafiullah Khan received his B.Sc. degree in Electrical Engineering from University of Engineering and Technology Peshawar, Pakistan, master degree in Satellite Navigation and Related Applications from Politecnico Di Torino, Italy, and Ph.D. degree jointly from University of Genoa, Italy and Polytechnic University of Catalonia, Spain, in 2009, 2010 and 2014, respectively. He completed his Ph.D. under a joint degree Erasmus Mundus program, funded by the European Commission. He is currently a postdoctoral research fellow at Queen's University Belfast in United Kingdom. He has co-authored over 35 scientific publications in international journals and conference proceedings and carried our research activities in framework of several national and European research projects. His research interests include Ad Hoc Networking, Cyber Security, Cyber Physical Systems and Critical Infrastructure Protection.

Sarmad Ullah Khan graduated in Electrical Engineering from University of Engineering and Technology, Peshawar, Pakistan in 2007. From 2007 to 2008, he was lecturer at CECOS university. In 2013, he received his PhD in Electronics and Telecommunication Engineering from the University of Politecnico di Torino, Italy. He is currently a postdoc research fellow at Politecnico di Torino, Italy. His research interests include security in wireless sensor networks, Internet of Things, intelligent transportation system and content centric networking.

Please cite this article as: R. Khan, S.U. Khan, Design and implementation of UPnP-based energy gateway for demand side management in smart grid, Journal of Industrial Information Integration (2017), http://dx.doi.org/10.1016/j.jii.2017.07.001